

1 Stephen R. Cochell (SBN 145225)  
2 *srcochell@gmail.com*  
3 COCHELL LAW FIRM, P.C.  
4 5850 San Felipe, Suite 500  
5 Houston, Texas 77057  
6 *Admitted Pro Hac Vice*

6 Allan Grant (SBN#213658)  
7 Grant's Law Firm  
8 17351 Greentree Drive  
9 Riverside, California 92503-6762  
Telephone (888)937-7555  
Facsimile (866)858-6637

10 Attorneys for Defendant  
11 JASON EDWARD THOMAS CARDIFF

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

14 UNITED STATES OF AMERICA,  
15 Plaintiff,  
16 vs.  
17 JASON EDWARD THOMAS  
18 CARDIFF,  
19 Defendant.

Case No. 5:23-CR-00021-JGB

[Filed concurrently with Declaration of  
Stephen R. Cochell, Jason Cardiff and  
[Proposed] Order]

Courtroom: 1  
Hearing Date: October 21, 2024  
Time: 2:00 PM

23 **DEFENDANT JASON CARDIFF'S NOTICE OF MOTION AND MOTION**  
24 **TO DISMISS COUNT TWO OF THE INDICTMENT**

## NOTICE

**TO ALL PARTIES AND ATTORNEYS OF RECORD:**

PLEASE TAKE NOTICE that on October 21, 2024, at 2 p.m. in the courtroom of the Honorable Jesus G. Bernal, United States District Judge, Defendant Jason Cardiff, by and through his attorneys of record, Stephen R. Cochell, hereby moves this Honorable Court for an order dismissing Count Two of the Indictment, which charges Aggravated Identity Theft, a violation of 18 U.S.C. § 1028A(a)(1).

This Motion is based upon the attached Memorandum of Points and Authorities, the Declaration of Stephen R. Cochell, the Declaration of Jason Cardiff, and all files and records in this case, and any further evidence as may be adduced at the hearing on this Motion.

This motion is made following the conference of counsel pursuant to L.R. 7-3, which took place on September 6, 2024.

Dated: September 9, 2024

By: /s/ Stephen R. Cochell  
Stephen R. Cochell

Attorneys for Defendant  
JASON EDWARD THOMAS CARDIFF

1 **TABLE OF CONTENTS**  
2

3	<b>NOTICE</b> .....	ii
4	<b>TABLE OF CONTENTS</b> .....	iii
5	<b>INDEX OF AUTHORITIES, MEMORANDUM OF POINTS AND</b> <b>AUTHORITIES</b> .....	iv
6	<b>I. INTRODUCTION</b> .....	1
7	<b>II. STATEMENT OF FACTS</b> .....	2
8	A. The Indictment.....	2
9	B. The FTC Action.....	3
10	C. The FTC's Statement of Uncontroverted Facts Relevant to Count One and Two of the Indictment.....	3
11	D. Redwood Did Not Store or Have Access to Customer Credit Cards, Debit Cards or Other Identifiers.....	4
12	<b>III. ARGUMENT</b> .....	6
13	A. Legal Standard.....	6
14	B. Count Two Must Be Dismissed Under the Supreme Court's Recent Decision in <i>Dubin</i> .....	8
15	<b>IV. CONCLUSION</b> .....	14
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 **INDEX OF AUTHORITIES**

2 **Case Law**

3	<i>Dubin v. United States</i> , 599 U.S. 110 (2023) .....	<i>passim</i>
4	<i>FTC v. Cardiff, et al.</i> , Case No. 5:18-CV-02104-DMG-PLA (C.D. Cal. 2018) .....	3
5	<i>U.S. v. Carter</i> , 2006 WL 997867 (E.D. Cal., Apr. 17, 2006) .....	7
6	<i>United States v. Felch</i> , No. 21-CR-0570, 2024 WL 406554, (D.N.M. Jan. 22, 2024) .....	13
7	<i>U.S. v. Jones</i> , 542 F.2d 661 (6th Cir. 1976) .....	6
8	<i>United States v. Mirabal</i> , 98 F.4th 981 (9th Cir. 2024) .....	7
9	<i>United States v. Noble</i> , No. 1:23-CR-00165-SDG, 2024 WL 253623, (N.D. Ga. Jan. 23, 2024) .....	13
10	<i>United States v. Ovsepian</i> , No. 21-55515 (9th Cir. September 3, 2024) .....	12-13
11	<i>U.S. v. Phillips</i> , 367 F.3d 846 (9th Cir. 2004) .....	7
12	<i>U.S. v. Rojas-Pedroza</i> , 716 F.3d 1253 (9th Cir. 2013) .....	7
13	<i>U.S. v. Shortt Accountancy Corp.</i> , 785 F.2d 1448v (9th Cir. 1986) .....	6
14	<i>United States v. Spears</i> , 729 F.3d 753 (7th Cir. 2013).....	10-11
15	<i>U.S. v. Van Griffin</i> , 874 F.2d 634 (9th Cir. 1989) .....	7
16	<i>U.S. v. Western Titanium, Inc.</i> , 2010 WL 3988291, (S.D. Cal., Oct. 12, 2010) .....	7

24 **Rules**

25	Fed. R. Crim. P. 12(b)(3)(B)(v) .....	2-3, 6
26	Fed. R. Evid 801(d)(2)(D) .....	7

1 **Statutes**

2 18 U.S.C. § 1028A(a)(1) ..... *passim*

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

## **MEMORANDUM OF POINTS AND AUTHORITIES**

## I. INTRODUCTION

4        The Indictment charges Mr. Cardiff with, among other things, Aggravated  
5 Identity Theft, a violation of 18 U.S.C. § 1028A(a)(1). After the Indictment was filed,  
6 the Supreme Court decided *Dubin v. United States*, 599 U.S. 110 (2023), which  
7 significantly narrowed the reach of the Aggravated Identity Theft statute. Applying  
8 *Dubin*, Mr. Cardiff’s prosecution for Aggravated Identity Theft cannot proceed, as his  
9 alleged conduct was the type of “garden variety” overbilling that the Supreme Court  
10 held was not penalized by the statute

11       A key component of aggravated identity theft, as clarified in *Dubin*, is the  
12 requirement of deception concerning "who" is involved in the transaction. The  
13 Supreme Court emphasized that identity theft occurs when a defendant uses another  
14 person's identification to deceive about the identity of the parties involved in the  
15 transaction. This means that the fraudulent use of identification must go to the heart  
16 of the deception, altering the perception of the identities of those involved. The crux  
17 of the healthcare fraud in *Dubin* was a misrepresentation about the qualifications of  
18 Dubin's employees. The *Dubin* court found that Dubin misrepresented how and when  
19 services were provided to a patient but he did not misrepresent *who* received the  
20 services. Thus, his use of a patient's identifying information did not fall within the  
21 meaning of § 1028A(a)(1). *Id.* at 132.

22 As in *Dubin*, there is no indication that Mr. Cardiff or Redwood Scientific  
23 Technologies used the customers' identities to deceive anyone about "who" was  
24 received the services. The identity of the customer as the purchaser and Redwood as  
25 the merchant remained clear and unaltered throughout the transactions. The alleged  
26 misconduct in this case pertains to "how" the transactions were processed, not to any  
27 misrepresentation of "who" was involved.

28 In addition to the fact that there was no misrepresentation as to the “who” in

1 the transactions in the instant case, the Government's § 1028A(a)(1) fails because  
2 neither Redwood nor Cardiff used credit card or debit card account numbers in the  
3 transactions. In *Dubin*, the Court rejected the Government's claim that Dubin's  
4 overbilling was facilitated by use of a Medicaid reimbursement number and therefore  
5 automatically fell within the definition of § 1028A(a)(1). *Id.* at 128. In this case, the  
6 credit card account numbers provided by Redwood customers were encrypted by a  
7 third party Customer Relationship Management ("CRM"). The account numbers were  
8 not accessible by Cardiff or Redwood staff. Unlike Mr. Dubin, who used Medicaid  
9 reimbursement numbers as an identifier, Redwood lacked access to customer credit  
10 card and debit card account numbers during January through April 2018.

11 The facts in this case fall squarely within the *Dubin* Court's analysis, holding  
12 that use of a means of identity (in that case Medicaid numbers) were simply a means  
13 to execute billing, but were not a tool for deception about the identity of the parties.

14 Accordingly, the Court should dismiss Count Two, which charges Mr. Cardiff  
15 with Aggravated Identity Theft.

16 **II. STATEMENT OF FACTS**

17 **A. The Indictment**

18 Mr. Cardiff is charged with three crimes: access device fraud under 18 U.S.C.  
19 § 1029(a)(5), aggravated identity theft under 18 U.S.C. § 1028A(a)(1), and witness  
20 tampering under 18 U.S.C. § 1512(b)(2)(B). (Indictment, Dkt. No. 1.) Only the first  
21 two offenses, contained in the first two counts, are relevant to this motion.

22 Count One, the access device fraud count, alleges that between January 22,  
23 2018 and May 2018, Mr. Cardiff effected transactions with debit and credit card  
24 account numbers and expiration dates belonging to Redwood customers, and in doing  
25 so, obtained at least \$1,000 during a one-year period.

26 Count Two, the aggravated identity theft count, alleges that between January  
27 22, 2018 and May 2018, Mr. Cardiff transferred, possessed, and used names, credit  
28 card account numbers, and debit card account numbers during and in relation to the

1 access device fraud count.

2 **B. The FTC Action**

3 As the Court knows, the government began its investigation of Mr. Cardiff's  
4 company Redwood Scientific Technologies, Inc. ("Redwood") through a civil  
5 investigative demand issued by the Federal Trade Commission ("FTC"). (*See Order*  
6 *Denying Defendant's Motion to Dismiss the Indictment*, Dkt. No. 79 at 2-9.) The FTC  
7 thereafter filed a civil action against various defendants, including Mr. Cardiff, his  
8 wife, and Redwood. *See FTC v. Cardiff, et al.*, Case No. 5:18-CV-02104-DMG-PLA  
9 (C.D. Cal. 2018) (hereafter cited as "*FTC v. Cardiff*" and referred to as "FTC  
10 Action"). The FTC eventually moved for summary judgment, and in doing so,  
11 submitted a "Statement of Uncontroverted Facts and Conclusions of Law" ("SUF").<sup>1</sup>  
12 *FTC v. Cardiff*, Dkt. No. 423-3 (Aug. 6, 2020). The FTC's SUF was cited extensively  
13 in the order granting in part the FTC's motion for summary judgment. *FTC v. Cardiff*,  
14 Dkt. No. 511 (Oct. 9, 2020).

15 **C. The FTC's Statement of Uncontroverted Facts Relevant to Count One  
16 and Two of the Indictment**

17 The SUF has a section titled "Jason Cardiff's 'Straight Sales-to-Continuity'  
18 Initiative." That section has factual allegations the FTC submitted to the court in the  
19 *FTC v. Cardiff* action ("FTC Facts"). Those same assertions constitute the conduct  
20 alleged in Counts One and Two of the Indictment.<sup>2</sup> The pertinent FTC Facts are as  
21 alleged as follows:

22 In January 2018, Mr. Cardiff purportedly directed that brand new continuity

23

---

24 <sup>1</sup> Because the SUF is 308 pages, Defendant has provided an extract of the relevant  
25 portions. Counsel is prepared to file the entire document if needed.

26 <sup>2</sup> The FTC Facts contained in the FTC's Statement of Uncontroverted Facts are accepted as true  
27 solely for the purpose of adjudication of the instant motion under Federal Rule of Criminal  
Procedure 12(b). Mr. Cardiff otherwise reserves the right to contest the FTC Facts at all stages of  
28 these proceedings and, indeed, does contest such alleged facts.

1 orders should be created for customers who had previously made one-time “straight  
2 sale” purchases so that their debit and credit cards could be charged again and going  
3 forward on a recurring basis. **Exhibit A**, Declaration of Stephen Cochell (hereafter  
4 “Cochell Dec.”) Ex. 1, SUF at ¶ 839. Redwood allegedly did not contact these  
5 consumers or get their approval for additional charges. **Exhibit A**, Ex. 1, SUF at ¶  
6 840. Redwood staff allegedly processed hundreds of these unauthorized transactions  
7 each day and reported their success and failure rates to Mr. Cardiff. **Exhibit A**, Ex. 1,  
8 SUF at ¶ 841.

9 The Government also alleges, in some cases, customers’ credit and debit cards  
10 had expired since their original orders had been placed. **Exhibit A**, Ex. 1, SUF ¶ 842.  
11 Mr. Cardiff allegedly directed his employees to try changing the cards’ expiration  
12 dates to see if that would allow the new charges to be processed. **Exhibit A**, Ex. 1,  
13 SUF ¶ 843.

14 The FTC further alleged that Redwood staff continued converting straight-sale  
15 customers to continuity plans and charging them without authorization until April  
16 2018. **Exhibit A**, Ex. 1, SUF ¶ 845. Redwood allegedly processed unauthorized  
17 charges for more than 1,500 consumers through Jason Cardiff’s straight-to-continuity  
18 initiative. **Exhibit A**, Ex. 1, SUF ¶ 847.

19 **D. PCI Compliance: Redwood Did Not Store or Have Access to  
20 Customer Credit Cards, Debit Cards or Other Identifiers.**

21 Payment card industry (PCI) compliance is mandated by credit card companies  
22 to help ensure the security of credit card transactions in the payments industry.<sup>3</sup> PCI  
23 Investopedia. Payment card industry compliance refers to the technical and  
24 operational standards that businesses follow to secure and protect credit card data  
25 provided by cardholders and transmitted through card processing transactions. *Id.*

26 \_\_\_\_\_  
27 <sup>3</sup> Defendant requests the Court take judicial notice of  
28 <https://www.investopedia.com/terms/p/pci-compliance.asp> which provides an  
overview of PIC compliance and will be cited as “PCI Compliance-Investopedia.”

1 Redwood customers engaged in transactions that were processed using a third-  
2 party Customer Relationship Management (CRM) system called Limelight, which  
3 was later known as “Sticky.” **Exhibit B**, Declaration of Jason Cardiff ¶ 3\_(hereafter  
4 “Cardiff Dec.”) Limelight provided CRM services provided that the customer was  
5 PCI compliant. **Exhibit B**, Cardiff Dec. ¶ 4 . When a Redwood customer purchased  
6 a product, the transaction was primarily conducted online, with customers entering  
7 their payment information directly into the Redwood website. **Exhibit B**, Cardiff Dec.  
8 ¶5. The credit card information was then tokenized and securitized. *Id.* at ¶ 5. Once  
9 the credit card number is entered and submitted, the credit card information is  
10 tokenized and securitized and cannot be accessed by redwood personnel. *Id.* at ¶4.  
11 Purchases could also be made through the phone room. *Id.* at ¶ 6 The order would be  
12 entered into the Sticky system and then tokenized and securitized. *Id.* at ¶ 5.

13 The CRM acknowledged the order was successfully placed, exports the data to  
14 the shipping department with the product, amount of product and where to ship the  
15 product. *Id.* at ¶ 8. While reports may be generated for each customer, the credit card  
16 information is redacted. *Id.* at ¶ 9.

17 During its investigation, the DOJ confirmed and amplified the above details.  
18 In an interview with the prosecutors and investigators in this case, Joanny Spina,  
19 Limelight’s Office Operation Manager, stated that banks send information to  
20 processing banks to approve or deny a sale. Notably, the “Sticky” CRM system  
21 adhered to PCI compliance standards, ensuring that credit card details were securely  
22 tokenized and inaccessible to any individual within Redwood or its associated entities.  
23 **Exhibit A**, Cochell Dec., Spina MOI, Ex. 2 at 2-3, **Exhibit A**, Bogosian MOI, Exhibit  
24 3 at 1 According Ms. Spina “Sticky”.io, “the system works with company call centers,  
25 payment gateways, and fulfillment providers, such as Shipstation (which printed  
26 labels for shipping). **Exhibit A**, Ex. 1 at 2. Credit card numbers are protected by  
27 encrypting the middle numbers of the card. “Sticky” sees the card as encrypted when  
28

1 extracting information" **Exhibit A**, Ex. 1 at 2.

2       The PCI compliance of the "Sticky" CRM system is akin to the secure  
3 transaction processing systems used by major online retailers such as Amazon. Once  
4 a customer's payment information is entered, it is immediately tokenized and  
5 securitized, rendering the actual credit card numbers inaccessible. This security  
6 measure ensures that even if overcharging occurred, it would not involve the  
7 unauthorized access or misuse of a customer's credit card details, as these details were  
8 never accessible to anyone within Redwood. This process was confirmed in the  
9 teleconference with "Sticky".io executives, where it was clarified that the system was  
10 structured to prevent access to sensitive customer information **Exhibit A**, Bagosian  
11 MOA, Ex. 3 at 1. Furthermore, Redwood also accepted payments through its phone  
12 room operations, where orders were similarly processed directly into the "Sticky"  
13 CRM system by phone representatives.

14       **III. ARGUMENT**

15       **A. Legal Standard**

16       "Rule 12(b) of the Federal Rules of Criminal Procedure permits any defense  
17 "which is capable of determination without the trial of the general issue" to be raised  
18 by pretrial motion." *U.S. v. Shortt Accountancy Corp.*, 785 F.2d 1448, 1452 (9th Cir.  
19 1986). "A pretrial motion is generally 'capable of determination' before trial if it  
20 involves questions of law rather than fact. *Id.* "However, 'a district court may make  
21 preliminary findings of fact necessary to decide the questions of law presented by pre-  
22 trial motions so long as the court's findings on the motion do not invade the province  
23 of the ultimate finder of fact.'" *Id.* (citing *U.S. v. Jones*, 542 F.2d 661, 664 (6th Cir.  
24 1976)). As such, Rule 12(b) allows a defendant may move to dismiss the pleadings  
25 on the basis of a "defect in the indictment or information" and a "failure to state an  
26 offense." Fed. R. Crim. P. 12(b)(3)(B)(v).

27       When a motion to dismiss an indictment is based on uncontested facts, the  
28 Court is "faced with a pure issue of law, which it ha[s] to decide because no good

1 cause existed to defer its ruling until trial.” *U.S. v. Phillips*, 367 F.3d 846, 855 (9th  
2 Cir. 2004); *see also Id.* at n. 25 (“Because neither party contested the facts, the district  
3 court neither ‘invade[d] the province of the’ jury nor determined an element of the  
4 offense.”), cited with approval in *U.S. v. Rojas-Pedroza*, 716 F.3d 1253, 1261 (9th  
5 Cir. 2013); *see also U.S. v. Carter*, 2006 WL 997867, at \*2 (E.D. Cal., Apr. 17, 2006)  
6 (“The existence of undisputed facts obviates the need for the district court to make  
7 factual determinations properly reserved for a jury.”).

8 For purposes of this Motion, and for the sake of argument, Cardiff assumes,  
9 that the FTC Facts proffered by the FTC in the FTC Action are true. Although “every  
10 publication of every branch of government of the United States” cannot “be treated  
11 as a party admission by the United States under Fed. R. Evid 801(d)(2)(D)[,]”  
12 statements made by a “relevant and competent section of the government” are  
13 admissible against the Government as an opposing party admission. *See U.S. v. Van*  
14 *Griffin*, 874 F.2d 634, 638 (9th Cir. 1989). In *Van Griffen*, the Ninth Circuit held that  
15 a pamphlet on sobriety testing created by the Department of Transportation (“DOT”)  
16 was admissible against the Government as a party admission. *Id.* Recently, the Ninth  
17 Circuit affirmed and clarified its holding in *Van Griffen*, explaining that the DOT’s  
18 statements were admissible against the Government because the prosecution involved  
19 a crime related to highway safety, which fell under the purview of the DOT. *See*  
20 *United States v. Mirabal*, 98 F.4th 981, 986 (9th Cir. 2024); *see also U.S. v. Western*  
21 *Titanium, Inc.*, 2010 WL 3988291, at \*8 (S.D. Cal., Oct. 12, 2010) (finding that  
22 Defense Contract Management Agency (“DCMA”))’s report may be admissible “as a  
23 party admission because the DCMA appears to be the relevant and competent  
24 government agency charged with the development of rules for defense suppliers to  
25 ensure that... supplies and services meet all performance requirements.”).

26 Just as the DOT was the “relevant and competent” agency of the Government  
27 related to crimes involving highway safety in *Van Griffen*, here the FTC is the  
28 “relevant and competent” agency of the government related to crimes related to

1 consumer protection. As such, the FTC Facts can be imputed to the government and  
2 because Cardiff does not dispute the FTC Facts for purposes of this Motion, the Court  
3 can consider whether the FTC Facts fail to state an offense as a matter of law.

4 Similarly, witness interviews conducted by the government are admissible if  
5 proffered by the defendant to support his defense. Rule 803(8), Federal Rules of  
6 Evidence allows for admission of factual findings from a legally authorized  
7 investigation when used against the government in a criminal case, and neither the  
8 source of information nor other circumstances indicate a lack of trustworthiness. In  
9 the instant case, the DOJ investigators and lawyers conducted an interview of Joanny  
10 Spina, an Operations Manager for LimeLight/Sticky, as part of their investigation of  
11 Defendant in this case.

12 **B. Count Two Must Be Dismissed Under the Supreme Court’s Recent  
13 Decision in *Dubin*<sup>4</sup>**

14 The aggravated identity theft statute provides that “[w]hoever, during and in

15  
16 <sup>4</sup> Moreover, the Aggravated Identity Theft statute is unconstitutionally vague. As Justice Gorsuch’s  
17 concurrence in *Dubin* explains, Section 1028A(a)(1) fails to provide even rudimentary notice of  
18 what it does and does not criminalize. *Id.* at 133. Because the terms “use” and “in relation to” can  
19 have numerous meanings and are not defined by the statute, individuals are left to guess about what  
“use” entails and what the necessary (or a fair) amount of relation to the enumerated offense is  
required. Such unconstitutional lack of clarity remains uncured by the majority opinion in *Dubin*.  
As Justice Gorsuch explains:

20 When, exactly, is a “means of identification” “at the crux,” “a key  
21 mover,” or a “central role” player in an offense? No doubt, the  
22 answer “turns on causation, or at least causation often helps to  
23 answer the question.” The Court agrees but stresses that “a causal  
24 relationship” of any kind will not suffice. At the same time,  
25 however, it studiously avoids indicating whether the appropriate  
26 standard is proximate cause or something else entirely novel. All of  
27 which gives rise to further questions. In virtually every fraud, a  
28 “means of identification” plays some critical role in the fraud’s  
success—good luck committing a mail or wire fraud, for instance,  
without relying heavily on the name of the victim and likely the  
names of other third parties. Just how much “causation” must a  
prosecutor establish to sustain a § 1028A(a)(1) conviction? For that  
matter, how does one even determine the extent to which a “means

1 relation to" certain enumerated felonies, "knowingly transfers, possesses, or uses,  
2 without lawful authority, a means of identification of another person, shall, in addition  
3 to the punishment provided for such felony, be sentenced to a term of imprisonment  
4 of 2 years." 18 U.S.C. § 1028A(a)(1). As relevant here, a means of identification  
5 includes names, credit cards, and debit cards.

6 The predicate felony charged in this case is access device fraud. That statute  
7 prohibits knowingly and with the intent to defraud, effecting transactions, with one or  
8 more access devices issued to another person or persons, to receive payment or any  
9 other thing of value during any one-year period the aggregate value of which is equal  
10 to or greater than \$1,000. 18 U.S.C. § 1029(a)(5)

11 The access devices used to effect the transactions alleged in Count One (access  
12 device fraud) are the credit and debit card numbers charged in Count Two (aggravated  
13 identity theft).

14 After the Indictment was returned, the Supreme Court reined in the  
15 government's sweeping interpretation and use of the aggravated identity theft statute  
16 in *Dubin*. The Court narrowly interpreted the statute as reaching more limited conduct  
17 than had previously resulted in convictions for aggravated identity theft, including  
18 convictions previously upheld in this circuit.

19 In *Dubin*, the petitioner overbilled Medicaid by inflating the qualifications of  
20 an employee who performed a test and claiming a higher reimbursement based on  
21 those qualifications. *Dubin*, 599 U.S. at 114. While the test had been done by a junior  
22 "psychological associate, the petitioner billed Medicaid as if the test had been done  
23 by a licensed psychologist. *Dubin*, 599 U.S. at 114. In the bill he submitted to

24  
25 \_\_\_\_\_  
26 of identification" "caused" an offense, as compared to the many  
27 other necessary inputs?

28  
29 *Id.* at 135 (citations omitted).

1 Medicaid, the petitioner included a patient’s name and Medicaid reimbursement  
2 number. *Dubin*, 599 U.S. at 115. Because he misrepresented the employee’s  
3 qualifications and overbilled Medicaid, the petitioner was convicted of the predicate  
4 offense of healthcare fraud. And because in the process of submitting the fraudulent  
5 bill, he used a “means of identification”—the patient’s name—he was also convicted  
6 of aggravated identity theft under § 1028A. *Dubin*, 599 U.S. at 114-15.

7 The Supreme Court reversed the petitioner’s conviction for Aggravated  
8 Identity Theft. In reaching its decision, the Supreme Court interpreted two provisions  
9 of the statute, “use” of another’s means of identification, and “during and in relation  
10 to” a predicate crime.

11 As to “use,” the Court reasoned that for someone to “knowingly … use[ ],  
12 without lawful authority, a means of identification of another person[,]” there must  
13 be deception going to “who” is involved in the transaction rather than just “how” or  
14 “when” services were provided. *Dubin*, 599 U.S. at 123. The Court explained that this  
15 is required because “identity theft is committed when a defendant uses the means of  
16 identification itself to defraud or deceive.” *Id.* In other words, when a means of  
17 identification is used deceptively, this deception goes to “who” is involved in the  
18 transaction, rather than just “how” or “when” services were provided. Use of the  
19 means of identification must be at “the locus of [the criminal] undertaking,” rather  
20 than merely ancillary to a crime. *Id.* at 123.

21 As for “in relation to,” the Court explained that the means of identification must  
22 play a “central role” or be a “key mover” in the predicate offense. “This central role  
23 played by the means of identification, which serves to designate a specific person’s  
24 identity, explains why we say that the ‘identity’ itself has been stolen.” *Id.* at 123  
25 (citing *United States v. Spears*, 729 F.3d 753, 756 (7th Cir. 2013) (“‘identity theft’  
26 occurs when someone’s ‘identity has been stolen or misappropriated’). Based on this  
27 reasoning, the Court explained why the below specific examples resulting from the  
28 Government’s interpretation of the statute did not sound like—and did not qualify

1 as—identity theft.

2 If a lawyer rounds up her hours from 2.9 to 3 and bills her  
3 client using his name, the name itself is not specifically a  
4 source of fraud; it only plays an ancillary role in the billing  
5 process. The same is true for the waiter who substitutes  
6 one cut of meat for another; we might say the filet  
7 mignon's identity was stolen, perhaps, but not the diner's.

8 *Id.* at 122–23 (emphasis added).

9 Therefore, the Court concluded, “a defendant ‘uses’ another person’s means of  
10 identification ‘in relation to’ a predicate offense when this use is at the crux of what  
11 makes the conduct criminal.” The Court clarified that this requires more than a “causal  
12 relationship,” such as facilitating the offense or being a but-for cause of its success.  
13 *Id.* at 131 (citing *Id.* at 135 (GORSLUCH, J., concurring in judgment)). Instead, the  
14 means of identification must be used in a manner that is in and of itself fraudulent or  
15 deceptive, going to “*who*” is involved in the transaction. *Id.* at 131–32.<sup>5</sup>

16 Turning to the FTC Facts, Mr. Cardiff’s misrepresentations went not to “*who*”  
17 he or Redwood was or “*who*” their customers were, but to the “*what*” and the  
18 “*when*”—i.e., whether the customer signed up for a one-time or monthly subscription  
19 for products sold by Redwood. In effectuating the alleged predicate crime of using  
20 the customers’ access devices to charge for monthly subscriptions when they had  
21 placed a one-time order, Mr. Cardiff did not misrepresent his or Redwood’s identity  
22 or use a customer’s means of identification that fraudulently or deceptively went to  
23 “*who*” was involved in the transaction. While using those customers’ names and credit

---

24 <sup>5</sup> In *United States v. Hong*, 938 F.3d 1040, 1050–1051 (9<sup>th</sup> Cir. 2019), the Ninth Circuit  
25 reversed a conviction for aggravated identity theft applying the circuit’s well-  
26 established rule interpreting the term “use” in limited context-specific ways. “To  
27 interpret ‘use’ broadly “could encompass every instance of specified criminal  
misconduct in which the defendant speaks or writes a third party’s name.” *Hong* at  
1051 citing *United States v. Spears*, 729 F.3d 753, 756 (7th Cir. 2013).

1 and debit card numbers was necessary to charge them for the subscriptions, that causal  
2 relationship is not sufficient under *Dubin*. If it were, there would be “an automatic 2-  
3 year sentence for generic overbilling that happens to use ubiquitous payment  
4 methods.” *Id.* at 129. *see also Id.* at 124 (decrying the government’s broad reading of  
5 the statute as applying an “aggravated” label “to all manner of everyday overbilling  
6 offenses” that would make “everyday overbilling” “the most common trigger for §  
7 1028A(a)(1)’s severe penalty”). Every offense of access device fraud, which  
8 necessarily requires the use of a person’s account numbers like credit cards and debit  
9 cards, could also be prosecuted as Aggravated Identity Theft. That would run afoul of  
10 the Supreme Court’s clear directive in *Dubin* to read the statute more narrowly than  
11 encompassing all ancillary features of billing using ubiquitous payment methods.

12 It would also make the “aggravated” part of the statute’s title irrelevant. In  
13 *Dubin*, the Court looked to the title of the statute as providing important context and  
14 color to the terms “uses” and “in relation to.” While the Court was careful to limit  
15 both the role that a title plays in statutory interpretation and the scenarios where a title  
16 may be relevant, it made clear that the Aggravated Identity Theft statute was one of  
17 those instances where its title provides meaningful—and determinative—context. *Id.*  
18 at 121-22. Significantly, the Court highlighted that Congress titled the criminal statute  
19 “Aggravated Identity Theft,” which it observed typically applies when an offense “is  
20 made worse or more serious by circumstances such as violence, the presence of a  
21 deadly weapon, or the intent to commit another crime.” *Id.* at 123. This suggests, the  
22 Court reasoned, that Congress had in mind “a particularly serious form of identity  
23 theft.” Permitting the government to tack on the 2-year mandatory minimum  
24 sentencing enhancement to what is a garden variety overbilling case would read  
25 “aggravated” out of the statute.

26 On September 3, 2024, the Ninth Circuit handed down its decision in *United*  
27 *States v. Ovsepian*, No. 21-55515. *Ovsepian* was a case where defendant allegedly  
28 “possessed” one patient file as part of an alleged conspiracy to commit health care

1 using Medicare and Medi-Cal identifying information. The Ninth Circuit reversed  
2 Ovsepian's 1028A conviction based on *Dubin*. In pertinent part, the Court reiterated  
3 that criminal liability under 18 U.S.C. § 1028A did not apply unless the use or  
4 possession of another's identifying information was at the "crux" of the fraudulent  
5 conduct, rather than an ancillary feature. *Ovsepian* at 25. The Court held that retention  
6 of a patient file may have been helpful in the event of an audit, but it was merely an  
7 "ancillary" feature of the scheme that merely facilitated its commission. *Id.* at 26  
8 citing *Dubin* at 132. In Mr. Cardiff's case, any use of customer credit card information  
9 was purely incidental to the alleged billing errors and did not constitute deception  
10 regarding "who" was involved in the transaction.

11       Multiple courts have resolved motions invoking *Dubin* to challenge aggravated  
12 identity theft prosecutions or convictions. The courts that have affirmed Aggravated  
13 Identity Theft convictions have typically involved cases where the defendants passed  
14 themselves off as another person—for example, by forging the signature of another  
15 person or applying for identity documents using someone else's identity—to defraud  
16 a third party like a bank or government office. *See, e.g., United States v. Felch*, No.  
17 21-CR-0570, 2024 WL 406554, at \*1–5 (D.N.M. Jan. 22, 2024) (upholding  
18 defendant's conviction for aggravated identify theft with a predicate offense of bank  
19 fraud where the defendant forged her employer's signature on a company check made  
20 payable to the defendant's credit card company). *Cf. United States v. Noble*, No. 1:23-  
21 CR-00165-SDG, 2024 WL 253623, at \*4–5 (N.D. Ga. Jan. 23, 2024) (holding that  
22 Section 1028A requires an identity to have been "stolen or misappropriated").

23       In contrast, here, the FTC Facts reflect that Mr. Cardiff did not pass himself off  
24 as another person. He did not misrepresent his identity. He did not hold himself out  
25 as a customer or anyone else using a customer's means of identification. He did not  
26 use the customers' means of identification to defraud or deceive third parties. He held  
27 himself out as a merchant of the goods that had, in fact, been purchased by the  
28 customers. He was himself, his customers were his customers; at most this was a

1 garden variety case of overbilling or overprocessing the credit and debit cards in  
2 question. Moreover, Mr. Cardiff did not possess any of the credit card or debit card  
3 information.

4 Mr. Cardiff's conduct cannot be meaningfully distinguished from the fact  
5 scenarios used by the Dubin court ruling out aggravated identity theft under the  
6 statute. For example, the lawyer who bills her client electronically for three hours  
7 when she only worked 2.9 hours. The lawyer charged her client's account, with the  
8 client's name and account number, to effectuate the fraud. And by doing so, the  
9 lawyer implicitly represented to the client that she had done three hours of work and  
10 represented to the bank that the client had authorized the transaction representing  
11 three hours of billable time. If, as the Supreme Court indicated, the lawyer did not  
12 commit aggravated identity theft, then Mr. Cardiff did not either. Mr. Cardiff used  
13 encrypted data provided by customers to the CRM which billed customers for  
14 monthly subscriptions even if some of the customers originally placed one-time  
15 orders. The encrypted data was necessary to effectuate the charges but use of the data  
16 was ancillary to the crux of any fraud.

17 As with the examples provided by the Supreme Court, Redwood's customers'  
18 names and the encrypted credit and debit numbers were ancillary features of billing.  
19 Those encrypted account numbers were certainly necessary to effectuate the  
20 transactions, as charged in Count One, but there was no act of deceit going to "who"  
21 was involved in the transaction. Reading *Dubin* to permit the government to proceed  
22 with an aggravated identity theft prosecution under these facts would be contrary to  
23 *Dubin*'s clear rejection of an overbroad reading of the statute. *See Id.* at 129 ("So long  
24 as the criteria for the broad predicate offenses are met, the Government's reading  
25 creates an automatic 2-year sentence for generic overbilling that happens to use  
26 ubiquitous payment methods.").

27 **IV. CONCLUSION**

28 In light of the Supreme Court's decision in *Dubin v. United States*, which

1 narrowed the interpretation of aggravated identity theft under 18 U.S.C. § 1028A, it  
2 is clear that Mr. Cardiff's alleged conduct does not meet the statutory requirements  
3 for aggravated identity theft. The *Dubin* Court held that, for a defendant to be  
4 convicted of aggravated identity theft, the misuse of a person's means of identification  
5 must be central to the fraudulent conduct.

6 In Redwood's case, the use of credit card numbers was not central to the alleged  
7 fraud. The *Dubin* decision made clear that for identity theft to occur, the misuse of  
8 identifying information must directly relate to the deception about "who" is involved  
9 in the transaction, not merely "how" the transaction is processed. In Redwood's case,  
10 the overcharging—if it occurred—did not involve the deceptive use of credit card  
11 numbers to misrepresent the identity of the parties involved. Instead, these credit card  
12 numbers were securely stored and never accessed, and the transactions in question  
13 were processed within the confines of a system designed to prevent unauthorized  
14 access to such sensitive information. This is further evidenced by the “Sticky”.io  
15 system's design, which explicitly prevented access to the underlying credit card  
16 information, as noted in the government's memorandum of activity.

17 The role of the credit card numbers in this situation were purely ancillary; they  
18 were necessary for processing payments, but they did not play a central, deceitful role  
19 in any alleged fraud. Any billing discrepancies that arose were related to the  
20 management of transactions, such as mistakenly placing customers on a recurring  
21 billing cycle, rather than to the misuse of a customer's identity.

22 This distinction is critical. Transactional errors, such as overbilling, are not  
23 equivalent to identity theft. Under *Dubin*, identity theft requires the misuse of a means  
24 of identification in a way that is fundamental to the fraud—something that did not  
25 occur in the operations at Redwood. Therefore, the conduct alleged in this case, even  
26 if proven, would not constitute aggravated identity theft, as the credit card numbers  
27 were not used in a manner that was central to any deceptive or fraudulent activity.

28

1 WHEREFORE, based on the foregoing, Mr. Cardiff respectfully requests that  
2 the Court dismiss Count Two of the Indictment with prejudice.

3 Respectfully submitted,

4 /s/ Stephen R. Cochell

5 Stephen R. Cochell

6 SBN: 24044255

7 The Cochell Law Firm, P.C.

8 5850 San Felipe, Ste 500

9 Houston, Texas 77057

(346) 800-3500 – Telephone

[srcochell@gmail.com](mailto:srcochell@gmail.com)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1 **SERVICE LIST**

2 I HEREBY DECLARE THAT THE FOLLOWING COUNSEL HAVE BEEN  
3 SERVED WITH THIS DEFENDANT JASON CARDIFF'S NOTICE OF MOTION  
4 AND MOTION TO DISMISS COUNT TWO OF THE INDICTMENT THROUGH  
5 THE COURT'S ECF OR NEXT GEN ELECTRONIC FILING SYSTEM:

6 E. Martin Estrada  
7 United States Attorney  
8 Mack E. Jenkins  
9 Assistant United States Attorney Chief, Criminal Division  
10 Ranee A. Katzenstein  
11 Assistant United States Attorney Chief, Criminal Division  
12 Valerie Makarewicz  
13 Assistant United States Attorney Major Frauds Section  
14 1100 United States Courthouse  
15 312 North Spring Street  
16 Los Angeles, CA 90012  
17 Telephone: (213) 894-0756 Facsimile: (213) 894-6269  
18 E-mail: [Valerie.Makarewicz@usdoj.gov](mailto:Valerie.Makarewicz@usdoj.gov)

19 Amanda Liskamm  
20 Director, Consumer Protection Branch Manu J. Sebastian  
21 Brianna M. Gardner  
22 Trial Attorneys  
23 Consumer Protection Branch  
24 U.S. Department of Justice  
25 450 Fifth Street NW, Suite 6400 Washington, DC 20001  
26 Telephone: (202) 514-0515 Facsimile: (202) 514-8742  
27 E-mail: [Manu.J.Sebastian@usdoj.gov](mailto:Manu.J.Sebastian@usdoj.gov)  
28 [Brianna.M.Gardner@usdoj.gov](mailto:Brianna.M.Gardner@usdoj.gov)

29 */S/ Stephen R. Cochell*  
30 Stephen R. Cochell